Service Name: OpenSSH (SSH)

Service Type: Vulnerable

Docker Image(s): tleemc2/metasploitable2

Intended Exposed Container Port: 22/tcp

Description & Rationale: OpenSSH is the standard secure shell service for remote administration. In Metaploitable2, the SSH service is intentionally left insecure by using weak/default credentials. This makes it an effective target for red team attacks, as they can perform password guessing/brute-force, credential stuffing, or replay of captured creds to obtain interactive shells. I choose SSH because it shows the real-word risk of poor credential configuration and weak access controls.

Service Name: Internal Database (PostgreSQL)

Service Type: Decoy

Docker Image(s): docker.io/library/postgres:15-alpine

Intended Exposed Container Port: 5432/tcp

Description & Rationale: PostgreSQL is a modern SQL database used in many production environments. Databases on run on port 5432 are common, and as a decoy, PostgreSQL provides a recognizable TCP fingerprint to port scanners while offering limited exploitation surface when configured with a strong password and no sensitive data. I choose PostgreSQL because it's a realistic internal service and often heavily targeted by attackers.

Service Name: Web Server (Nginx)

Service Type: Decoy

Docker Image(s): docker.io/library/nginx:latest

Intended Exposed Container Port: 80/tcp

Description & Rationale: An up-to-date Nginx web server is extremely common in production. So running a server on 8080 as the host looks legitimately to attackers doing reconnaissance. It attracts attackers into doing HTTP probes, directory discovery, and using automated scanners while limiting exploit surface is kept current. I chose Nginx because it is customizable and useful as a honeypot.

Network Name: nexus_net

Port Mapping Strategy:

- OpenSSH: 22/tcp → 2222/tcp
- Nginx: 80/tcp → 8080/tcp
- PostgreSQL: 5432/tcp → 5432/tcp